ARTIFICIAL INTELLIGENCE POLICY

1. GENERAL PROVISIONS

Approved at the 16th Extraordinary Meeting of the Board of Directors (BoD), held on December 11, 2025 (Version 1).

This Policy will be reviewed at least every two (2) years, or at any time when it is necessary to adapt it to legislative changes or other relevant facts affecting its content. The policy review will require prior communication with the areas responsible for maintaining the relevant standards so that these can be revised while remaining consistent with the new policy.

2. PURPOSE

The purpose of this Artificial Intelligence Policy is to establish definitions, principles, guidelines, and responsibilities to be observed for the development, governance, implementation, and responsible use of artificial intelligence systems at Sanepar, aiming to protect fundamental rights, guarantee the implementation of safe and reliable systems, promote technological innovation and the efficiency of services in an ethical, transparent, and equitable manner with human supervision and audit mechanisms.

3. SCOPE

This policy applies to everyone who interacts with artificial intelligence systems for corporate activities at Sanepar, including administrators, members of the Supervisory Board and Committees, employees, interns, apprentices, third parties, and all individuals with whom Sanepar interacts or has a relationship. This includes both internally developed AI systems and those provided or operated by third parties and used by the Company.

This Policy is available at the following web address: https://ri.sanepar.com.br/governanca-corporativa/estatuto-codigos-e-politicas and, once approved by the Board of Directors, it must be disclosed to all persons who must comply with it.

4. REFERENCES

4.1 Bill No. 2338/2023 (it provides for the use of Artificial Intelligence);

4.2 Regulation (EU) 2024/1689 (Artificial Intelligence Regulation);

4.3 CNJ Resolution No. 615/2025 (it provides for solutions developed with artificial intelligence resources)

4.4 ABNT ISO 19.011 – Guidelines for auditing management systems;

4.5 ABNT ISO 38.507 – Information Technology – IT Governance – Governance implications of the use of artificial intelligence by organizations;

4.6 ABNT ISO 27.037 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence

4.7 ABNT (Series) ISO 27.000 – Information technology - Security techniques - Information security management systems - Overview and vocabular;

This Policy should be read and interpreted in conjunction with current legislation, the Articles of Incorporation, other corporate policies, with special attention to the Information Security Policy, the Personal Data Protection and Privacy Policy, the Information Protection Regulation, and the Sanepar Code of Conduct and Integrity, ensuring an integrated approach to governance and security.

5. DEFINITIONS

The terms and expressions mentioned in this Policy are listed in Table 1. When used within the scope of Sanepar's Artificial Intelligence Policy, they will have the following meaning:

Table 1 - Terms and Definitions of the Artificial Intelligence Policy

Term	Definition
Hallucination	Generating information that appears plausible but is factually incorrect, inconsistent, or fabricated by the AI system;
Audit	A systematic, independent, and documented process for obtaining data that objectively evaluates the artificial intelligence system, to determine the extent to which the set of pre-established requirements is met;
Life Cycle	Evolution of a system, product, service, project, or other entity developed by humans, from conception to its decommissioning;

Table 1 - Terms and Definitions of the Artificial Intelligence Policy

(continuation)

Term	Definition
Fundamental Rights	These are guarantees provided for in the 1988 Federal Constitution that ensure the dignity of the human person, freedom, equality, privacy, and other essential values. They represent limits to the power of the State and guide the ethical conduct of public and private institutions.
Discrimination	Any distinction, in the area of public or private life, whose purpose or effect is to nullify or restrict the exercise, under conditions of equality, of one or more rights provided for in the legal system, based on personal characteristics such as geographic origin, race, color or ethnicity, gender, sexual orientation, socioeconomic class, age, disability, religion or political opinions;
Explainability	The property of an artificial intelligence system to express crucial factors that influence the results of the artificial intelligence system in a way that humans can understand;
Risk	Deviation from the expected uncertainty in the objectives;
Artificial Intelligence System	A computational system that uses machine learning-based approaches, capable of creating results such as content, predictions, recommendations, or decisions, given a specific set of objectives defined by humans. A computational system that uses approaches based on logic, knowledge, and machine learning, capable of producing results such as content, predictions, recommendations, or decisions that influence physical or virtual environments, with varying levels of autonomy and in view of a specific set of objectives defined by humans.
Supervision	Monitoring the implementation of organizational and governance policies and managing associated tasks, services, and products determined by the organization, to adapt to changes in internal or external circumstances;
Use of Artificial Intelligence System	To develop or apply an artificial intelligence system through any part of its lifecycle to fulfill the organization's objectives;
Bias	Systematic difference in the treatment of particular objects, people or groups compared to others.

6. PRINCIPLES

This policy should serve as a guide for the development of internal rules on matters that may affect the development, governance, implementation, and use of artificial intelligence systems, aiming to guarantee the principles presented in Table 2:

Table 2 - Principles governing the use of artificial intelligence systems

Principles	Definition
Auditability	The artificial intelligence system should enable an independent assistant or other authorized interested party to evaluate the activities performed;
Human Centricity and Human Supervision	The artificial intelligence system should be designed and operated to serve human well-being, always ensuring the possibility of adequate human supervision and intervention;
Reliability	The artificial intelligence system must consistently satisfy a stated, usually implicit or mandatory, need or expectation;
Controllability	The artificial intelligence system should allow a human being or other external agent to intervene in the system's operation;
Explainability	The artificial intelligence system must express crucial factors that influence its results in a way that humans can understand;
Non-Discrimination	The artificial intelligence system must ensure fair and equal treatment for all individuals affected by its results;
Predictability	The artificial intelligence system should allow for reliable assumptions about the outputs by any relevant individual, group, or organization that may affect, be affected by, or perceive themselves as affected by an outcome;
Robustness	The artificial intelligence system must be able to function reliably and consistently in different scenarios, handling disturbances, errors, and incomplete or noisy data without compromising its performance or security;
Security	The artificial intelligence system must be secure, resilient to attacks and errors, and protected against vulnerabilities that could compromise data integrity or decision-making, preventing physical, psychological, or material harm.
Sustainability	The development and use of artificial intelligence systems should consider and minimize their environmental impact, including energy and resource consumption, promoting sustainable practices;
Transparency	The artificial intelligence system must make the necessary information about the system available to any relevant individual, group, or organization that may affect, be affected by, or perceive themselves as affected by an outcome.

7. GUIDELINES

This Artificial Intelligence Policy establishes general guidelines related to the fundamental rights of affected individuals, risk classification, governance, transparency, and data use. Furthermore, it defines specific guidelines for generative artificial intelligence solutions, as described below:

7.1. FUNDAMENTAL RIGHTS

In the development, deployment, and use of artificial intelligence systems, the Company must ensure that these tools are compatible with fundamental rights. To guide this alignment, the following specific guidelines should be followed:

I. To verify compliance with fundamental rights at all stages of an artificial intelligence system's lifecycle, assessing and mitigating potential risks;
II. To implement audit and monitoring mechanisms to ensure that artificial intelligence systems remain in compliance with fundamental rights and the guidelines of this Policy;
III. To ensure that the results generated by artificial intelligence systems preserve equality, non-discrimination, and plurality;
IV. To implement preventive measures to avoid the emergence of results with discriminatory biases;
V. To adopt corrective measures if the results show discriminatory biases or are incompatible with the proposed solution; and
VI. To provide internal and external communication channels that address potential complaints from individuals affected by high-risk artificial intelligence systems.

7.2 RISK CLASSIFICATION

In the development, deployment, and use of artificial intelligence systems, the Company must conduct a thorough assessment to classify the level of risk associated with each solution properly. To do this, the following specific guidelines must be followed:

I. Authorize the use of artificial intelligence systems only after they have been approved in accordance with Company's regulations;
II. To assess artificial intelligence systems to define their risk level, based on the categorization provided in Annex I of Risk Classification;
III. To determine the reclassification of the artificial intelligence system whenever there is any change that indicates an alteration in risk;

IV. To implement continuous monitoring mechanisms to ensure compliance with prohibitions on artificial intelligence systems that do not allow for human supervision or present excessive risk; and
V. To monitor and periodically review artificial intelligence systems to ensure they remain within their categorization parameters.

7.3 GOVERNANCE

In the development, deployment, and use of artificial intelligence systems, the Company needs to establish effective governance. This governance should ensure that AI is aligned with the company's objectives and that all security requirements are met. To do this, the following specific guidelines must be observed:

I. To publish reports detailing the operation, data used, oversight mechanisms, and decisions involved in building artificial intelligence systems, whether contracted or developed by the Company, throughout their entire lifecycle;
II. To utilize tools that facilitate integration or interoperability between other systems, whenever technically feasible and in accordance with information security and privacy requirements;
III. To utilize tools or processes for automatically recording the operation of high-risk artificial intelligence systems, whenever technically feasible;
IV. To adopt measures that enable the explainability of high-risk artificial intelligence systems, whenever technically possible;
V. To conduct periodic algorithmic impact assessments for high-risk artificial intelligence systems, as regulated by relevant legislation;
VI. To subject high-risk artificial intelligence systems to regular auditing processes and continuous monitoring to oversee their use and mitigate risks; and
VII. To adopt the principle of segregation of duties in the development, training, validation, and deployment phases of artificial intelligence systems, to minimize the possibility of undetected errors, fraud, and biases, in accordance with the Company's internal control guidelines.

7.4 TRANSPARENCY

The Company has a duty to ensure the transparency of artificial intelligence solutions at all stages, including their development, deployment, and use. To do so, you must observe and comply with the specific guidelines that will be detailed below:

I. Issue periodic reports demonstrating compliance with the guidelines of this policy;

II. Adopt measures that enable the explainability of artificial intelligence systems, so that decisions, operations, and results are understandable to users and auditable; and

III. To register, openly to the public, the high-risk artificial intelligence systems developed, implemented and used by the Company, along with their respective preliminary assessments, when required by applicable law.

7.5 DATA

The Company must ensure that, in the development, deployment, and use of its artificial intelligence solutions, all legal and regulatory data-related obligations are observed. Furthermore, it is essential to adopt appropriate practices for all operations, following the specific guidelines that will be presented:

I. To document clearly, traceably, and transparently the fulfillment of obligations related to the data lifecycle, storage, sharing, privacy, security, retention, and disposal of data, as stipulated in the company's Policies and standards;

II. To ensure that all data processing operations, such as annotation, labeling, cleaning, enrichment, and aggregation, are aligned with the specific purpose for which the data is being used;

III. To conduct periodic assessments of the availability, quality, volume, adequacy, and representativeness of data before using them for any operation;

IV. To ensure that the data used comes from secure and reliable sources and is accurate, relevant, up-to-date, and representative of the affected populations, tested against discriminatory biases, anonymized whenever possible, undergoes curation and monitoring processes, and observes precautions regarding protections, restrictions and confidentiality, intellectual property, judicial secrecy, and the protection of corporate and personal data;

V. To confirm that the storage and execution of artificial intelligence systems occur in environments that meet information security standards, ensuring isolation and protection against risks of destruction, alteration, loss, or unauthorized access and transmission of data;

VI. To ensure that data management measures used in artificial intelligence systems mitigate and prevent discriminatory biases, and process data in accordance with the Personal Data Protection and Privacy Policy, the Information Security Policy, and the Information Protection Regulation; and

VII. To ensure that data held by the Company is not shared with artificial intelligence solutions accessed through websites, applications, or application programming interfaces (APIs) not contracted, except when such data has been previously anonymized or pseudonymized at the source, in accordance with the General Data Protection Law (LGPD) and best information security practices.

7.6 GENERATIVE ARTIFICIAL INTELLIGENCE

The company must establish rigorous criteria for the use of generative artificial intelligence at all stages — development, deployment, and use. This includes defining specific restrictions and obligations applicable to both internal and external third-party solutions. The following specific guidelines should guide the construction of this governance:

I. To provide users with training on best practices, limitations, risks, and the ethical, responsible, and efficient use of generative artificial intelligence;
II. To ensure that the use of generative artificial intelligence occurs only as support for human activities, prohibiting its use as an autonomous tool;
III. To prohibit the use of generative artificial intelligence for purposes deemed excessively risky and high-risk;
IV. To prohibit the use of confidential data for training and processing generative artificial intelligence models;
V. To ensure that the use of confidential data in processing within generative artificial intelligence systems can be achieved through adjustments that prevent the compilation of the generative artificial intelligence knowledge base;
VI. To seek to inform about the use of generative artificial intelligence in all products developed primarily through the tool's decision-making process;
VII. To ensure that the contractor does not use the data provided by the Company for training and improvement of external generative artificial intelligence or artificial intelligence unrelated to the contracted object, or for any other purpose not expressly authorized, and must act in accordance with current legislation;
VIII. To ensure that the contractor safeguards the confidentiality of data and information, and that audits or reports may be required at any time;
IX. To ensure that the contractor has up-to-date system documentation; and
X. To ensure that the contractor adopts privacy and security measures from the design stage and as standard in its systems.

8. RESPONSIBILITIES

This Policy establishes the responsibilities for the Board of Directors, Executive Board, Information Security Committee, Technical Information Security Committee, Structures and Management, and Users, as listed below:

8.1 Board of Directors

I. To approve the Artificial Intelligence Policy;

II. To resolve on matters about their responsibilities.

8.2 Executive Board

I. To promote the process of complying with approved guidelines and ensure that they are aligned with good management practices, including the Company's strategic planning;

II. To resolve on the procedures referred by the Deputy Executive Board of Governance, Risks and Compliance, in the event of incidents;

III. To submit to the Board of Directors, for approval, proposals for revising this policy and specific cases that involve strategic decisions;

IV. To ensure the alignment of planning actions, promoting the necessary adjustments through standardized operating procedures in their respective executive boards.

8.3 Information Security Committee

I. To discuss and deliberate on content related to artificial intelligence, as well as to define strategic guidelines and orientations related to the topic;
II. To determine the classification and assess the need for reclassification of artificial intelligence systems;
III. To consolidate governance standards and risk mapping that enable compliance with this policy;
IV. To assess the suitability of using artificial intelligence systems that the Company could employ;
V. To monitor training and development opportunities related to artificial intelligence;
VI. To determine the need for or establish the frequency with which audits and monitoring actions of artificial intelligence systems should be carried out, as well as to define and implement standardized technical audit protocols;
VII. To support audit actions to assess adherence to this policy in the Company's areas, contributing with recommendations for improvement, and providing process feedback;
VIII. To establish transparency standards.

8.4 Information Security Technical Committee

I. To discuss and resolve on the technical content related to artificial intelligence, as well as to define strategic guidelines and orientations related to the topic;
II. To be consulted on the analysis and classification, and to assess the need for reclassification of artificial intelligence systems;
III. To be consulted on governance standards and risk mapping that enable compliance with this policy;
IV. To evaluate technical infrastructure and development issues related to the use of artificial intelligence systems that could be implemented in the Company;
V. To monitor training and development opportunities related to artificial intelligence;
VI. To be consulted on recommendations regarding the execution and frequency of audits and monitoring actions of artificial intelligence systems, as well as to define and implement standardized technical audit protocols;
VII. To support the auditing of artificial intelligence systems, ensuring that they remain compliant with fundamental rights, compatible with the proposed solution, and mitigate potential risks related to the systems;
VIII. To contribute to defining transparency standards upon request from the Information Security Committee.

8.5 Structures and Management

I. To standardize the processes related to their area of operation, observing this and other Company policies;
II. To provide information on Sanepar's Artificial Intelligence Policy, according to its scope;
III. To periodically provide training and guidance on concepts, rules, and procedures applicable to artificial intelligence, both in general corporate terms and specific to its activity.
IV. To periodically provide training and guidance to users regarding concepts, rules, and procedures applicable to artificial intelligence, both in general corporate terms and specific to their activity.

8.6 User

I. To be responsible for guiding, interpreting, verifying, and reviewing the information contained in the results obtained by artificial intelligence systems, to mitigate risks arising from hallucinations;
II. To provide training on best practices, limitations, risks, and the ethical, responsible, and efficient use of artificial intelligence systems.

9. ACCOUNTABILITIES

9.1 Failure to comply with the responsibilities set forth in this Policy must be reported to both the Information Security Committee and the Risk Management and Compliance Department and will be dealt with in accordance with the provisions of the Sanepar's Code of Conduct and Disciplinary Regulations, without prejudice to the application of other rules governing information security and labor relations.

9.2 Failure to comply with the provisions of this Policy and other regulations relating to Artificial Intelligence may result in disciplinary measures under Sanepar's Integrity Program, regardless of administrative, civil, and criminal liability.

10. FINAL PROVISIONS

Any questions regarding the interpretation of this Policy may be addressed to the Deputy Executive Board of Governance, Risk and Compliance – Data Protection Officer.

This policy becomes effective on the date of its approval by the Board of Directors.

HISTORY

INFORMATION SECURITY POLICY			Version	1st
			Management Area	DAGRC
			Confidential	External Public
Version	**Date**	**Person-in-charge**	**Approved by:**	**Description of the Change**
1st	12/11/2025	Deputy Executive Board of Governance, Risk and Compliance	Board of Directors	Initial Issue